EXHIBIT 1

05/27/2016

[redacted]

USA vs Roman Seleznev
Analysis in Response to Defense Expert Reports & Opinions as of May 27, 2016

A digital investigative analysis methodology designed to stay within the authorized scope of the investigation and minimize analyst exposure to files and information was used. This report contains only the most significant digital artifacts necessary to satisfy the interrogatories of the analysis within the time allotted, based on the investigative information and tools available to the analyst at the time of the analysis. Additional artifacts may be provided upon further analysis or additional request.

DOJ CCIPS Cybercrime Lab
Response to Defense Report

Analyst: Ovie Carroll, Director, DOJ Cybercrime Lab, Computer Crime and Intellectual Property Section
Report Date: April 1, 2016

Executive Summary

On request of Assistant United States Attorney Seth Wilkinson, a digital investigative analysis was conducted on the forensic image of a Sony VAIO computer identified as belonging to Roman Seleznev. An analysis was requested to address the issues raised by defense expert from Blank Law + Technology P.S. for United States of America v. ROMAN SELEZNEV (W.D. WA, Case No. CR11-0070RAJ), Credit Card Theft / Computer Hacking, dated March 1, 2016. The main issue requested to be addressed was the post-seizure activity on the computer. The following items of interest were found:

Based on an analysis of the forensic image of the Sony VAIO computer hard drive, it is my opinion that the evidence clearly indicates that the post-seizure activity is not attributable to any user tampering with files. Evidence shows that file timestamp changes after 7/5/2015 were the result of McAfee and other system related programs conducting routine maintenance operations while the computer was in a low-power state. A thourgh review of the files with timestamps changed subsequent to law enforcement's seizure of the device do not diminish or negatively impact the integrity of the system.

A digital investigative analysis methodology designed to stay within the authorized scope of the investigation and minimize analyst exposure to files and information was used. This report contains only the most significant digital artifacts necessary to satisfy the interrogatories of the analysis within the time allotted, based on the investigative information and tools available to the analyst at the time of the analysis. Additional artifacts may be provided upon further analysis or additional request.

Detailed Findings

OPINION

A. The computer was not connected to any wireless or wired network after the device was seized. Remote data access was not possible; therefore no data alteration occurred or was possible via remote access over a network.

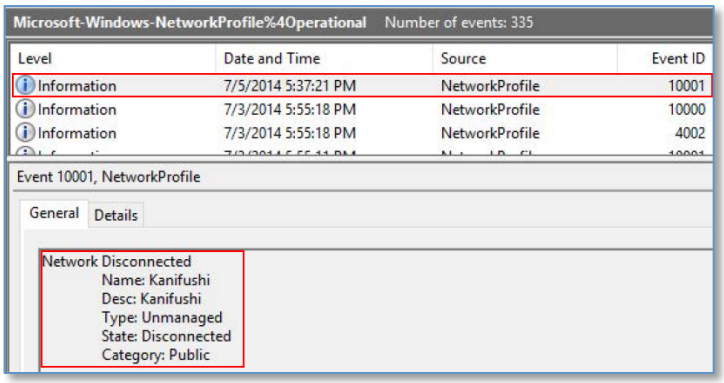
There are multiple digital forensic artifacts maintained automatically by the Windows operating system that track every network connection. Analysis of those artifacts clearly shows the computer last connected to a network named Kanifushi on 7/3/2014 at 21:55 (UTC). It did not connect to any other networks after this. As shown by multiple digital artifacts in the following section, the computer did not connect to any wireless or wired networks at any time after the device was seized. Although the device was not completely powered down after seizure, the lack of any network connection ensures that no files or communications were sent to the computer over a network. So regardless of the amount of protection from wireless communications, the state of the computer was not affected by any wireless communications.

BASIS FOR OPINION

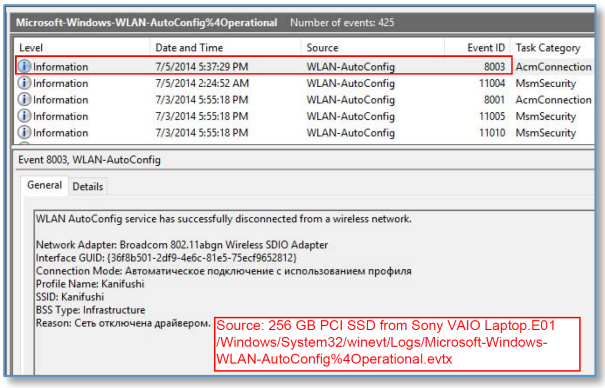
1. There are two primary Windows registry keys that record and maintain a list of every wired or wireless network the Windows 8 operating system connected to, including the first and last time each network connected. A review of the SOFTWARE registry hive, as shown in **Attachment-1-Network Registry Key.pdf**, shows the last network this device connected to was a network named Kanifushi on 7/3/2014 at 17:55 (UTC).

2. Windows 8 maintains several event logs in which every network the computer system connects to is recorded. A review of these event logs shows the last network this computer connected to was the Kanifushi network.

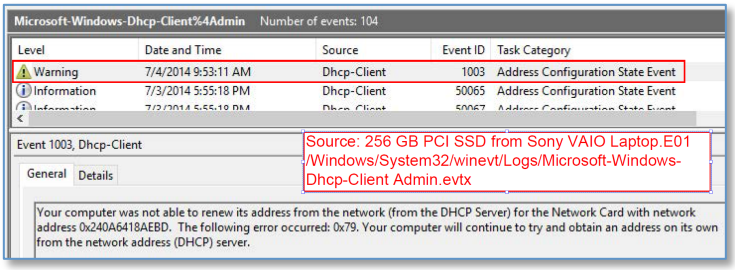
   a. The last entry in the "Network Profile Operational" event log recorded at 7/5/2014 at 17:37:21 (UTC) as event ID 10001 that the operating system no longer had an established connection with the Kanifushi network as shown in **Attachment-2-Network Profile Operational Event Log.pdf**. If this computer had connected to any other network subsequent to the Kanifushi network, this log would have recorded it.



b. The last entry in the "WLAN AutoConfig Operational" event log recorded at 7/5/2014 at 17:37 (UTC) as event ID 8003 that the operating system successfully disconnected from the Kanifushi network as shown in **Attachment-3-Microsoft Windows WLAN AutoConfig Operational Event Log.pdf**. If this computer had connected to any other network subsequent to the Kanifushi network, this log would have recorded it.



c. The last entry in the "Microsoft Windows DHCP Client Admin" event log recorded a Warning event as event ID 1003 indicating the computer was no longer able to renew its IP address from the DHCP server as shown in **Attachment-4-Microsoft Windows DHCP Client Admin Event Log.pdf**. If this computer would have connected or attempted to connect to another DHCP network in order to receive an IP address, this log would have recorded it.



3. By default, the Windows Update Client records transaction information to the Windows Update.log file. The last entry in this log that shows the network state as "Connected" is dated 7/5/2014 at 05:09:42 (UTC). All subsequent recorded network states in this log show as "Disconnected." The Windows update log file, as shown in **Attachment-5-WindowsUpdate.pdf**, further supports and corroborates the above information that the computer was not connected to a network after 7/5/2014. The Windows Update Client records when the operating system checks for updates from Microsoft servers and records the network state for each instance. If this computer had connected to a network subsequent to 7/5/2014 and the Windows Update Client had attempted to check for updates from the Microsoft server, the connect state would have been recorded as "Connected."

4. The above documented digital artifacts negate the suggestion that this device may have connected to a network while the screen appeared off because of the Windows 8 feature called Connected Standby. The Connected Standby[1] feature was enabled on this computer as evidence by the CsEnabled registry key located in the SYSTEM registry hive attached as **Attachment-6-CsEnabled Regisry Key.pdf**. When a computer is in Connected Standby, the screen may appear off but the operating system continues to perform several system functions. However, a system in Connected Standby may connect to a network **only** if that network is a previously known trusted network.[2] Furthermore, digital artifacts exist on the system that record changes while the computer is in Connected Standby. As previously stated above and as shown in **Attachment-1-Network Registry Key.pdf**, an examination of this system shows the last network this system connected to was the Kanifushi network on 7/3/2014 at 17:55 (UTC). This

[1] Connected standby is also known as InstantGo and Modern Standby.
[2] https://msdn.microsoft.com/en-us/library/windows/hardware/mt637223(v=vs.85).aspx

system recorded at 7/5/2014 at 17:37 (UTC) in event id 8003 that it successfully disconnected from the Kanifushi network, as shown in **Attachment-3-WLAN AutoConfig Operational Event Log.pdf**. Therefore, while in Connected Standby the computer did not connect to any network after the device was seized by law enforcement.

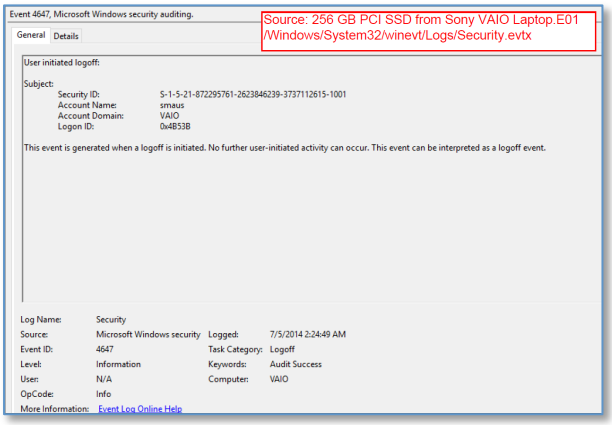
OPINION

B. None of the file creation, access, and modification timestamp activity subsequent to 7/5/2014 was a result of a user being logged into the computer. Analysis shows that the last user account to log into the computer was an account named SMAUS and that user logged out of the computer at 7/5/2014 at 2:24 (UTC). No other user account logged into the computer either directly or remotely after 7/5/2014 at 2:24 (UTC). All changes in timestamps were a result of system processes and not any user account.

The digital artifacts detailed in this section are automatically created and record changes to files in the Windows 8 operating system. Analysis of these artifacts shows that all of the activity on the computer that occured after the seizure of the device is due to system processes, and not by a user who gained access to the computer via local or remote access.

BASIS FOR OPINION

1. The Security event log, as shown in **Attachment-7-Security Event Log.pdf**, maintains a record of account logon and logoff activity. The Security event log shows user SMAUS logged off the computer on 7/5/2014 at 2:24 (UTC). The log entry states that "*No further user-initiated activity can occur*." There are no logons by SMAUS or any other users after this. All subsequent activity is the result of standard system services, not human access.



2. The System Resource Usage Monitor (SRUM) is a feature of the Windows 8 operating system that monitors applications, system services, energy usage, and network activity and records it hourly in a database called SRUDB.DAT. As shown in **Attachment-8-SRUM Report.pdf**, this database records all processes run and identifies the user account (by security identifier) responsible for the activity. The last application activity recorded by SRUM attributed to a user account was the TOR Browser which was recorded at 7/5/2014 at 2:24 (UTC), and the user account responsible for the activity was identified as security identifier "S-1-5-21-872295761-2623846239-3737112615-1001," which belongs to the SMAUS user account. All application activity recorded subsequent to 7/5/2014 at 2:24 was not attributed to a user account but rather to system accounts. The system accounts included security identifiers:

- S-1-5-18 (a service account that is used by the operating system),
- S-1-5-19 (local service),
- S-1-5-20 (network service), and
- S-1-5-90 (DWM-2 Window Manager).[3]

SRUM Report

AutoIncId	UTC TimeStamp	AppId	UserId	ForegroundCycleTime
114124	07/05/2014 02:24:00	\Device\HarddiskVolume5\Users\smaus\Desktop\Tor Browser\Browser\firefox.exe	S-1-5-21-872295761-2623846239-3737112615-1001	98131300135
114125	07/05/2014 02:24:00	\Device\HarddiskVolume5\Users\smaus\Desktop\Tor Browser\Tor\tor.exe	S-1-5-21-872295761-2623846239-3737112615-1001	12666306444
114126	07/05/2014 18:00:00	System	S-1-5-18	399250986 76
114127	07/05/2014 18:00:00	\Device\HarddiskVolume5\Windows\System32\smss.exe	S-1-5-18	6248861
114128	07/05/2014 18:00:00	\Device\HarddiskVolume5\Windows\System32\csrss.exe	S-1-5-18	1481443719
114129	07/05/2014 18:00:00	\Device\HarddiskVolume5\Windows\System32\wininit.exe	S-1-5-18	22530756
114130	07/05/2014 18:00:00	\Device\HarddiskVolume5\Windows\System32\winlogon.exe	S-1-5-18	433206023

3. The Update Sequence Number Journal (aka: USN Journal, USN Change Journal and $UsnJrnl) is a feature of the Windows 8 operating system which records file activity. When any change is made to a file or directory, the USN journal is updated with a description of the change and the name of the file or directory. The USN Journal is analogous to the black box flight recorder on airplanes in that, depending on the level of activity, it generally maintains a record for one to two weeks. The most recent recorded file activity was dated 7/14/2014 at 00:36:23. **Attachment-9-USNJournal Post Logoff.pdf** is a section of the USN Journal showing file activity that was recorded after the user account SMAUS last logged off on 7/5/2015 at 2:24 (UTC) (see #1 above). A review of file activity recorded in the USN Journal subsequent to 7/5/2014 proves no file activity is attributed to user files, and rather the activity on the system is consistent with system maintenance functions.

4. The McAfee antivirus program runs automatically without user interaction and attempts to scan files on the computer system to detect viruses or malware. Two process related to the McAfee antivirus suite are known as "McAfee Service Host" and "McUpdate.exe." These processes create logfiles named "McSvHost###.log" and "McUpdate###.log." The earliest record in the McUpdate000.log file is 5/15/2014 at 6:19:21PM (Moscow Time), and the last entry recorded is at 7/7/2014 at 11:47:59PM. The earliest record in the McSvHost000.log file is 7/11/2014 at 4:00:41AM and the last entry recorded in the McSvHost002.log is at 7/14/2014 at 04:35:52AM. This shows that the antivirus program was another service running on the computer subsequent to its seizure which accounts for file timestamp changes. These log files are included in **Attachment-10-McAfrr Logs.zip**.

5. As stated above, the Windows Update Client log also recorded that the operating system continued to run and attempt to perform system updates after the device was seized on 7/5/2014, which accounts for file timestamps being updated.

6. Mr. BLANK's statement on page 3 of Document 388, Reply Re Motion To Suppress-1 filed 5/23/2016 that the SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon registry key and "$UsnJrnl" entries indicate that a user logged on to the "smaus" Windows user account and clicked past the Windows lock screen on July 7, 2014 at 19:46 UTC is an incorrect understanding or interpretation of the meaning of the registry key. Mr. Blank provided a

[3] See Microsoft knowledgebase article KB243330, "Well-known security identifiers in Windows operating systems," for more information about these security identifiers.

screenshot where he highlighted the "LastUsedUsername" value and the registry key Last Written Time and stated this value was proof a user logged on to the SMAUS Windows user account on July 7, 2014 at 19:46 UTC. Mr. Blank's conclusion is incorrect. The Winlogon registry key contains several values (24 values in this instance) that can be updated by various Windows events. The last written time of any registry key reflects the last time a value in that registry key is updated. In this specific instance, as the other related Windows artifacts support, the last written time of the Winlogon registry key was not a result of a user logging into the system.

OPINION

C. A thorough analysis of this computer shows that the integrity of the digital evidence on this system is intact, and there is no evidence or indication of tampering with the file system or user files. As described by the below digital artifacts, the access timestamps being updated on the LNK files in the user SMAUS profile folder is not, as the defense expert suggests, evidence of file tampering or any other nefarious activity.

It is a widely accepted understanding in the digital investigative analysis profession that there are too many variables that affect the Last Accessed timestamps to render them significant to any forensic examination. Creation and Modified times are significantly more reliable and are generally relied on during digital investigative analysis and typically the basis for any conclusions or opinions of temporal activity. Furthermore, the files the defense examiner brought into question with Last Accessed dates after 7/5/2014 do not have modified dates after the computer was seized on 7/5/2014, except in the case of the McAfee antivirus program files, Sony VAIO diagnostic files, SRUM database, Windows Diagnostics, and other system-related programs. The changes to the file access timestamps are consistent with McAfee and other system related programs conducting routine maintenance operations, which updated last access times.

BASIS FOR OPINION

---

1. The McAfee antivirus program, Sony VAIO diagnostics, SpyHunter malware scanner, Google Update and other system-related programs run automatically without user interaction and attempt to scan files on the computer system.

    a. The USN Journal log shows that the McSvHost001.log file was being updated 60 seconds before and 120 seconds after the LNK files' Last Accessed times were updated. The McSvHost001.log file being written to is evidence that the McAfee antivirus program was active and running at the time.

    b. The System Resource Usage Monitor (SRUM) log file recorded that the McAfee antivirus program, Sony VAIO diagnostic programs, SpyHunter malware scanner, Google Update and other system-related programs were active and running subsequent to the device seizure and through the Last Accessed timestamps being changed. This

explains and is consistent with the LNK file Last Accessed timestamps being updated. The SRUM does not show any user files or indicate that the contents of the files were changed after seizure.

2. The defense expert suggests that someone may have attempted to run live digital forensic tools, such as the ones mentioned by the defense expert or any other live forensic tool, on the system before the search warrant was obtained or at some point prior to the forensic image being created on August 1, 2014. If this had happened, a plethora of digital artifacts would have been created and evident on the system, to wit, the SRUM, USN Journal log, Windows Prefetch, several Windows Registry keys, Setupapi.dev.log file, system event logs, and pagefile.sys to name a few. No evidence exists at all to show that any live forensic tool was run on the system.

3. Finally, to the defense expert's suggestion that someone may have conducted wholesale copying of files, as documented above, no user logged in to the computer subsequent to the user account SMAUS logging off on 7/5/2014. No network connection was established subsequent to device seizure. Therefore, no one could have locally or remotely conducted wholesale copying of files to or from the system.

OPINION

D. The evidence shows the Sony Vaio was never shutdown while in law enforcement custody prior to August 1, 2014, and remained in a low power Connected Standby state. Mr. BLANK's statement in paragraph 19 and 20 of his declaration that the computer was last shutdown on July 14, 2014 is incorrect and the evidence plainly refute Mr. BLANK's conclusions and assertions.

The examiner's documented observation of the splash screen being displayed is consistent with the functionality of the Windows Connected Standby feature and is consistent with the digital evidence found during the analysis of the Sony Vaio. Although MR. BLANK is correct in his statement in paragraph 18 of his declaration that "*Windows event logs record computer startup and shut down, and many other activities. There are no event log entries on the laptop for August 1, 2014.*" MR. BLANK is plainly incorrect in his conclusion that "*…there is no possibility that a splash screen was displayed…*". The examiners observation of the splash screen being displayed is consistent with the functionality of the Windows Connected Standby feature.

BASIS FOR OPINION

---

1. When a Windows computer goes through the shutdown process there are several digital artifacts that log the shutdown event date and time. The two most common digital artifacts used in digital investigative analysis to document when a system is shutdown is the Windows System Event Log ID 6006 (identifying the event log service was stopped) and the "LastShutDown" registry key value in the System registry hive.

a. An examination of the evidence reveal the last Event log ID 6006 was recorded on June 27, 2014 at 11:32:42 UTC as seen in **Attachment-11-Windows System Event Log ID 6006.pdf**.

b. The LastShutDown registry key value in the System registry hive recorded the last shutdown time as "CE D0 9C 85 FB 91 CF 01" which is a Windows 64-bit Hex Value (Little Endian) for June 27, 2014 at 11:32:48 UTC as seen in **Attachment-12-LastShutDown.pdf**.

c. The Windows System event logs also recorded the system had two subsequent "unexpected" shutdowns (likely a system crash) on the same date (June 27, 2014) at and 15:59:31 and 16:40:01 as recorded in event ID 6008. Both of these artifacts are documentation and evidence that the last time the device went through the shutdown process was June 27, 2014.

2. There was no evidence to support this system either went through the shutdown process or experienced an unexpected shutdown on July 14, 2014. Mr. BLANK is incorrect in his conclusion that "*…there is only log activity to support the conclusion that the computer powered off July 14, 2014, and never restarted*" as Mr. BLANK stated in paragraph 19 and 20 of his declaration.

3. Mr. BLANK's statement in paragraph 17 that the few files with modification or access dates of August 1, 2014 and the lack of evidence of the computer going through the startup process after July14, 2014 is evidence that the Sony Vaio never went through the shutdown process or experienced an unexpected shutdown while in law enforcement custody. The files with timestamps of August 1, 2014 are addressed in a subsequent opinion in this report.

OPINION

E. The files with timestamps of August 1, 2014 were created or modified as a part of the Sony Improvement Program and consistent with the system momentarily transitioning from Connected Standby to an active state.

Mr. BLANK stated in paragraph 17 of his declaration that *"The few files that are accessed or modified on August 1, 2014…'seem consistent' [emphasis added] with an orphaned SSD being connected externally to another computer (like a forensic imaging machine)…".* Mr. BLANK's assertion is incorrect and suggests a lack of understanding of the Connected Standby feature introduced in Windows 8. MR BLANK's statement is also not consistent with Windows file system operations.

BASIS FOR OPINION

1. The files with timestamps of August 1, 2014 were part of the Sony Improvement Program, which runs routinely as a scheduled task. The Sony Improvement Program task initiated immediately upon the computer transitioning from Connected Standby to an active state after receiving a wake event input from the keyboard, button or touchscreen.

2. In order for the Sony Improvement Program files to be created or modified on August 1, 2014, the Sony Improvement Program must be running, the Windows operating system must have been in an active state (having not been shut down) and the hard drive must be in the Sony Vaio computer. The creation and modification of the Sony Improvement Program files on August 1, 2014 is evidence the hard drive was not removed from the computer and connected to another computer system as suggested by Mr. BLANK, but that the operating system was still running and had never been shutdown on July 14, 2014.

3. The files with timestamps of August 1, 2014 occurred approximately 23 minutes before the forensic imaging audit log recorded that the image of the Sony Vaio initiated and is consistent with the investigators documented actions and observations that caused the splash screen to be displayed and the fact that the operating system was still running and had never been shutdown on July 14, 2014.

4. As further evidence for this opinion, the Sony Improvement Program configurations.xml file was modified on August 1, 2014 to reflect that the next runtime of the Sony Improvement Program was scheduled for August 3, 2014 at 01:48:46. It is implausible to suggest the any other action other than what was stated by the agent would have modified the Sony Improvement Program configuration.xml file and scheduled the next runtime of the Sony Improvement Program. This is further evidence that the operating system was running and not shutdown on July 14th as Mr. BLANK stated.

OPINION

F. The actions of the investigative examiner to connect power to the Sony Vaio on or about July 30, 2014 was justifiable if the investigator was going to attempt to image RAM.

BASIS FOR OPINION

1. The criminal scheme being investigated and alleged of the defendant requires an enhanced degree of technical knowledge, awareness of covert communication protocols and an intentional effort to maintain operational and communication security (OPSEC and COMSEC). Based on my training and experience conducting digital investigations, an investigator would expect to encounter levels of encryption to include whole disk encryption. A review of some of the

investigative examiner's emails revealed he sent an email on July 30th articulating he had purchased a near identical Sony Vaio computer and was performing tests on the test system to determine if RAM imaging was possible. If an investigator believed the drive was encrypted, an advance investigative step would be to attempt a live image of RAM to recover the Windows password. To do this the computer would need to be powered and awake.

a. Based on the email communications of the investigative agent, subsequent to plugging the seized computer into A/C power the agent conducted several tests on a duplicate test computer and determined the likelihood of successfully obtaining an image of RAM was unlikely. The agent abandoned his idea of attempting to image RAM on the seized computer and never conducted or attempted any such attempt.

2. In order for the agent to attempt to image RAM he would have been required to insert some form of portable storage into the seized computer. Having charged the seized computer battery, this action would have triggered a wake event and caused the computer to transition out of Connected Standby into an active state and would have caused numerous changes to the Windows registry, event logs and a significant number of files. An analysis shows no such activity occurred. The lack of any such changes to the system, registry and event logs is evidence no attempt to image RAM was conducted.

It is my opinion and I am confident that all the data on the computer hard drive are valid and have not been tampered with. The way the computer was handled did not cause and does not constitute data tampering.

Ovie Carroll
Director Cybercrime Lab
Department of Justice Criminal Division
Computer Crime and Intellectual Property Section

Evidence Examined

Forensic Image of Sony VAIO computer identified as belonging to Roman Seleznev

Filename: 256 GB PCI SSD from Sony VAIO Laptop.E01
Verification MD5 Hash: a63554a0dcfcec2567072ed07fd16aa2

Forensic Tools Used During Examination

- AccessData FTK
- AccessData Registry Viewer
- TZWorks web suite
- Triforce ANJP-v3.13.0_201509141000_x64
- SrumMonkey
- Decode SRUM (05 June 2015)
- DCode v4.02a